**Procedural Standard 04-1**

**July 22, 2013**

TO: All DES Staff

FR: Gus Adams, Director, Disability Evaluation Services

BY: William Lewis, Associate Director, Administration and Finance (DES Compliance Coordinator)

RE: **DES Data Protection Policies and Procedures**

**Re: Data Security Breach and/or Inadvertent Disclosure of Personally Identifiable Information (PII) including Protected Health Information (PHI)**

**Applicability:**

For the purposes of this policy, the Disability Evaluation Services (DES) workforce shall include all DES employees as well as certain other personnel, such as contractors and/or subcontractors, consultants, interns, and volunteers, who perform services for DES, either on the premises of DES, or at some other remote location.

All workforce members must follow these policies and procedures.

**Purpose:**

State and federal laws and regulations, as well as agreements with clients and owners of PII and PHI, obligate DES to protect the confidentiality and security of PII/PHI. Failure to comply with such obligations may result in financial penalties, costs imposed to notify consumers, and reputational harm.

This purpose of this standard specifies responsibilities of DES workforce members, and places them on notice of potential disciplinary actions and sanctions in the event of an inadvertent disclosure and/or data security breach involving PII.

**Definitions:**

For the purpose of this policy, the terms member or client will refer to an applicant, current member or client, former member or client or deceased member or client, or recipient of any program affiliated in any way with DES.

Personally Identifiable Information (PII) includes Protected Health Information (PHI). PII applies when DES holds data identifying an individual (including applicants and employees) by first and last name, or first initial and last name, in combination with one or more of the following: Social Security Number; driver’s license number; state-identification card number; financial account number or credit or debit card number.

PHI means any individually identifiable information regarding a member’s or client’s health, health care or payment for health care, whether in electronic or non-electronic format.

PHI includes a member’s name or social security number, as well as a member's DES case/episode numbers, a member's birth date and date(s) of involvement with DES, diagnosis, claims history, or any part of a member's home address (including town or zip code) or telephone or cellphone number(s).

Aggregate data is also considered PHI unless it is stripped of all identifiers, including geographic subdivisions smaller than a state, all dates other than years, and all zip codes except the first three numbers.

**Inadvertent Disclosure of PII/PHI**

If it is suspected or known that an inadvertent disclosure of PHI occurs, whether verbal or written, it must be reported immediately to the workforce member’s Supervisor, the DES Compliance Liaison, and Commonwealth Medicine Office of Compliance & Review (CWM OCR) for special handling.

Examples of inadvertent disclosure of PII/PHI include but are not limited to:

Transmission of non-secure email

Faxing PHI to the wrong fax number

Improper disposal of PHI

Improper protection of case files (leaving files in inappropriate areas)

Improper verification of recipient’s identification

Documents containing PHI mailed to the wrong address

**Data Security Breach of PII/PHI**

If it is suspected or known that a data security breach of the electronic data systems used by UMass, CWM and/or DES, our subcontractors, or our customers involving PII/PHI has occurred, it must be reported immediately to the workforce member’s Supervisor, the DES Compliance Liaison, and CWM OCR for special handling.

Examples of a data security breach of PII/PHI include but are not limited to:

Loss or theft of a computer, laptop, smart phone, or other mobile device containing PII or PHI

Loss or theft of a portable storage device (external hard drive, thumb drive, etc) containing PII or PHI

Loss or destruction of paper case files transported or located off site

**Procedure:**

**Staff Responsibilities:**

In the event that an inadvertent disclosure of PII/PHI is discovered (through whatever means, i.e. staff discovery, phone call from recipient of disclosure, letter, etc.) staff must:

1. Notify their manager and/or the DES Compliance Liaison immediately upon discovery of the inadvertent disclosure.
2. Take all possible steps to retrieve the PII/PHI (if sent in error to an external source) for review and destruction.
3. Notify their manager and/or the DES Compliance Liaison of the outcome of retrieval efforts.

Failure to comply with the policies and procedures set forth in this Procedural Standard may result in disciplinary action, up to and including termination of employment. In some circumstances, violations may be grounds for civil action or criminal prosecution. In addition, DES may be liable for any penalties imposed by the US Department of Health and Human Services Office of Civil Rights in regard to the inadvertent disclosure.

**DES Management Responsibilities:**

Upon notification of an inadvertent disclosure the manager and/or DES Compliance Liaison will:

1. Immediately complete (on the same day as the notification from the staff member) Attachment A, Disclosure Risk Assessment Checklist and e-mail to [compliance@umassmed.edu](mailto:compliance@umassmed.edu) with a cc: to the DES Compliance Liaison. If all of the information requested is not available yet, submit the checklist anyway and e-mail a fully complete copy as soon as possible afterwards.
2. Mail Attachment B, Confirmation of Destruction form, to the recipient of the inadvertent disclosure for them to complete and mail back to the manager or DES Compliance Liaison. Upon receipt of the completed form, the manager or DES Compliance Liaison will forward the form to CWM OCR. In the event the form is not returned, inform CWM OCR, who will then follow up with the recipient.
3. The manager supervising the staff person responsible for the inadvertent disclosure will review the incident and take necessary corrective action, which may include:
   1. Retraining
   2. Review of process to determine any corrective root cause issues
   3. Close supervision as indicated
   4. If warranted, disciplinary action up to and including termination of employment

**Summary:** Changes in federal and state laws require the updating of DES procedures regarding inadvertent disclosures and data breaches of PI/PHI. As described in this PS, DES staff is responsible to immediately report such incidents and to attempt to recover the documents and/or document their safe destruction by the recipient. DES is also required now to report on the outcome of correction and notification efforts and provide follow up systems analysis and training to prevent future occurrences.

**Confirmation of Destruction: To Individual that received information in error from UMMS**

**Please choose the appropriate option below, complete and return the form.**

Please return form via   
 email: laurie.richard@umassmed.edu  
 *or* fax: 508-856-6060  
 *or* mail: Laurie Richard  
 Office of Compliance and Review  
 333 South St.  
 Shrewsbury, MA 01545

**Documents received in error by Mail:**

I have been in contact with University of Massachusetts Medical School and I confirm that the documents I received in error on (please enter date) \_\_\_\_\_\_\_\_\_\_ were:

shredded in a way that personal information cannot practically be read or reconstructed  
  returned to UMass Medical School  
  other (please specify)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Where were the documents stored upon receipt? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Did anyone else have access to or view the documents?  Yes  No

Name(s) of person(s) viewing documents: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Documents received in error by Fax:**

I have been in contact with University of Massachusetts Medical School and I confirm that the documents that I received in error by fax on (please enter date) \_\_\_\_\_\_\_\_\_\_ were:

shredded in a way that personal information cannot practically be read or reconstructed  
  returned to UMass Medical School  
  other (please specify)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Where was the fax stored upon receipt? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Did anyone else have access to or view the fax?  Yes  No

Name(s) of person(s) viewing fax: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Email received in error:**

I have been in contact with University of Massachusetts Medical School and I confirm that the email and any attached documents I received in error on (please enter date) \_\_\_\_\_\_\_\_\_\_ were:

deleted from my inbox and my deleted mail  
 deleted from my inbox, my sent mail (if a reply was made), and my deleted mail  
 other (please specify)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Furthermore, I confirm that:  
  I did not open or view the documents  
  the email was not forwarded

Did anyone else have access to or view the email?  Yes  No

Name(s) of person(s) viewing email: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Additional Comments, if any

I declare to the best of my knowledge and belief that the information I have provided is true, correct, and complete.

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name of business: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Is this business a Covered Entity or a Business Associate under the HIPAA Rule?

Yes  No

Address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

City, State, Zip Code: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Phone number: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**INSTRUCTIONS**

1. CWM workforce members observing an actual or potential disclosure of PHI or PI (referenced as PI) must first immediately inform their supervisor.
2. After informing their supervisor, workforce members and/ or their supervisor should complete only the blue fields of this checklist.
3. The Breach Risk Assessment Checklist must be emailed to [compliance@umassmed.edu](mailto:compliance@umassmed.edu). **The Disclosure Risk Assessment Checklist** **must be submitted on the same day on which the potential disclosure is observed. If all the information requested is not available yet, submit the checklist anyway.**
4. DO NOT include any Protected Health Information or Personal Information on the Checklist.

|  |  |
| --- | --- |
| Name of workforce member reporting disclosure: |  |
| Phone number/ email: |  |
| Business Unit: |  |
| Name of workforce member involved in the disclosure: |  |
| Name of supervisor of workforce member involved in the disclosure: |  |
| Date disclosure occurred: |  |
| Date disclosure discovered: |  |
| Data owner of data disclosed: (Ex.: MassHealth, NHP, DTA) |  |
| Contract name or number under which we received the data: |  |
| Name of affected individual(s) whose PI was disclosed? (This information is needed for tracking purposes and must be included.) |  |
| List of **ALL** data elements used or disclosed:  (Examples: member name, date of birth, Medicaid number, insurance number, address, etc.) |  |
| Was disclosure a limited data set? (Did it exclude date of birth and zip code?) | Yes  No |
| If data disclosed is not immediately identifiable does recipient have ability to re-identify data? | Yes  No |
| Was inadvertent disclosure due to the release of more than minimum necessary information? | Yes  No |
| Are data elements particularly sensitive? (for example mental health, HIV, or substance abuse) | Yes  No |
| Do elements increase risk of identity theft or financial fraud?  If clinical information, could data be used in a manner adverse to the individual or to further the unauthorized recipient’s own interests? | Yes  No  Yes  No  N/A |
|  | |
| Brief description of how disclosure occurred: |  |
| How did CWM learn of the disclosure? |  |
| Name of individual or entity receiving disclosure: |  |
| Information about the recipient or location if known. For example, a health care provider, attorney’s office, a MassHealth member, unrelated business office, etc. |  |
| Address/Fax # of individual/ entity receiving disclosure: |  |
| Was PI actually acquired or viewed? If no, explain.  Examples: letter returned unopened, email deleted without being viewed. | Yes  No |
| What mitigation measures were taken to recover data or verify destruction? List steps taken and when. |  |
| What assurances were received that recipient will destroy or return the PI? |  |
| What mitigation measures were taken to prevent a similar disclosure recurring in the future? |  |
| Does unauthorized recipient have obligations to protect privacy and security of the information under HIPAA? | Yes  No |
| Does unauthorized recipient have obligations to protect privacy and security of the information under other federal or state law? (specify) | Yes  No |
| Did impermissible use or disclosure of PI result in PI leaving the premises or crossing the firewall? | Yes  No |
| Specify the degree of confidence we have in the recipient’s assurances that they will destroy or return the PI. | High  Low  Explain: |
|  | |
| Were assurances received that recipient destroyed or returned the PI sufficiently comprehensive? | Yes  No  Explain: |
| Disclosure risk analysis (Enter investigation notes, including potential harm to affected individual(s) and potential risk to CWM/others.): |  |
| Action to be taken: | To be resolved by CWM Privacy Officer  Additional workforce training needed  Review/ update procedures (specify below)  Employee sanctions (specify below)  Other (specify below)  No Action Required |
| Is a report to data owner required? | Yes  No  If yes, complete the 2 boxes below. |
| Date reported to data owner: |  |
| To whom was disclosure reported and how was it reported? |  |

| Communications | | | | |
| --- | --- | --- | --- | --- |
| **Date** | **Delivered By/ Organization** | **Mode** | **Received By/ Organization** | **Summary of Communication** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

*\*\*\*End of Document\*\*\**